PROTECTIVE MEASURES INFRASTRUCTURE CATEGORY: HIGHER EDUCATION INSTITUTIONS

Protective Measures Section
Protective Security Division
Department of Homeland Security

Version: September 13, 2006

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO).** It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document will be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

For more information about this document contact:
Wade Townsend (703-235-5748 Wade.Townsend@dhs.gov)

PROTECTIVE MEASURES
INFRASTRUCTURE CATEGORY:
HIGHER EDUCATION INSTITUTIONS

Protective Security Division
Department of Homeland Security

Reducing the nation's vulnerability to acts of terrorism by protecting our critical infrastructures and key assets from attack is a core homeland security mission. Meeting the requirements of this mission means building and fostering a collaborative environment in which federal, state, and local governments and the private sector can better protect the infrastructures and assets they control. This report focuses on protective measures for one critical infrastructure sector: higher education institutions. The report is one of a series of documents that characterize and discuss the protective measures that are available to selected infrastructures. Other related reports on higher education institutions are also available that provide information on common vulnerabilities and potential indicators of terrorist activity. Collectively, these documents are designed to increase awareness and collaboration and to provide a foundation for detailed protective measures planning.

POTENTIAL THREATS

Protective measures are employed in response to various threats to:

- Increase awareness among site managers and law enforcement agencies,
- Reduce vulnerabilities of sites and their respective critical assets, and/or
- Enhance the defense against and response to an attack.

As such, it is important to understand terrorist objectives and the types of threats to our country's critical infrastructures and key assets, which include higher education institutions.

Terrorist Objectives

In general terms, terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States in order to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence. Figure 1 depicts the range of possible objectives for a terrorist attack on higher education institutions. Inflicting casualties in the form of fatalities, injuries, and illnesses is one of the major objectives of many terrorist acts. Casualties can occur both at the targeted facility and in the surrounding area. Damage or destruction of the facility can be intended either to shut down or degrade the operation of the facility or to cause the release of hazardous materials to the surrounding area. Disruption of the targeted site without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. Theft of equipment, materials, or products can be intended to divert these items to other uses or to reap financial gain from their resale. Theft of information can be intended either to acquire insight that is not public information or to gain data that can be used in carrying out attacks.

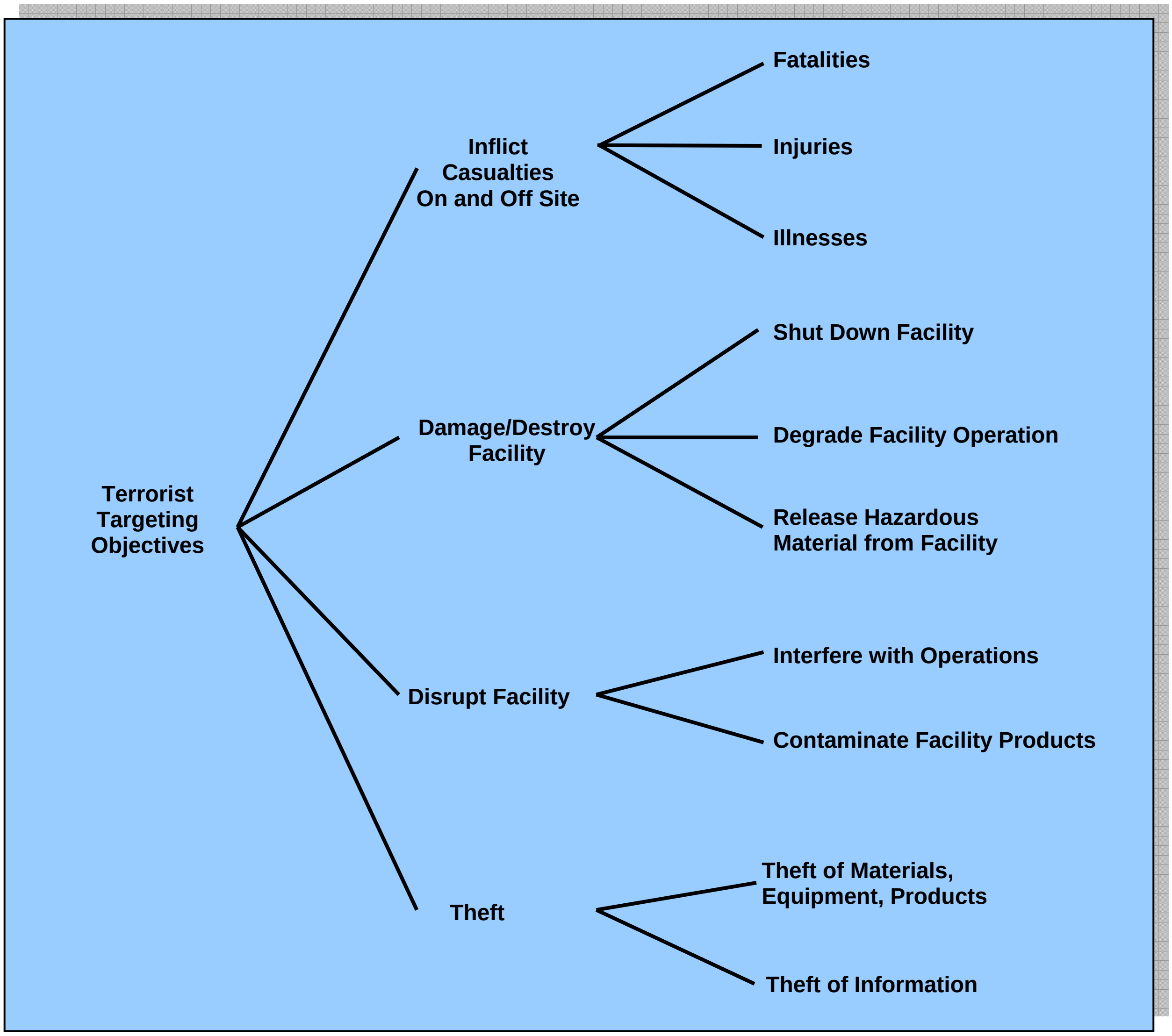
Terrorist Targeting Objectives
Inflict Casualties On and Off Site
Fatalities
Injuries
Illnesses
Damage/Destroy Facility
Shut Down Facility
Degrade Facility Operation
Release Hazardous Material from Facility
Disrupt Facility
Interfere with Operations
Contaminate Facility Products
Theft
Theft of Materials, Equipment, Products
Theft of Information

Figure 1 Potential Terrorist Targeting Objectives

Threat Categories

Terrorists have a variety of weapons and tactics available to achieve their objectives and have demonstrated the ability to plan and conduct complex attacks, simultaneously, against multiple targets. Attacks can be carried out by individuals, small teams of a few perpetrators, or larger groups acting in a coordinated fashion. Some of the many potential categories of threats (threat streams) of concern are described in the following sections.

Improvised Explosive Device (IED)

Explosives are a common weapon used by terrorists. They range from small explosive devices detonated by a lone suicide bomber to large quantities of explosives packed into a car or truck (vehicle-borne improvised explosive devices [VBIEDs]) or water-borne craft (water-borne improvised explosive devices [WBIEDs]). There are an increasing number of coordinated bombing attacks around the world.

Chemical Attack

Chemicals can be exploited or used by terrorists as a weapon. Such chemicals include toxic industrial chemicals (e.g., chlorine, ammonia, hydrogen fluoride) and chemical warfare agents (e.g., sarin, VX).

Biological Attack

Biological pathogens (e.g., anthrax, botulin, plague) can cause disease and are attractive to terrorists because of the potential to cause mass casualties and to exhaust response resources.

Nuclear/Radiological Attack

Although weapons-grade nuclear material is relatively difficult to obtain, some sources of nuclear and radiological material are more readily available (e.g., from medical diagnostic equipment) and easier to deliver than others in the form of a radiological dispersal device.

Aircraft Attack

Both commercial and general aviation aircraft can be used to deliver attackers, explosives, or hazardous materials; they can also be used as weapons.

Maritime Attack

Ships and boats of various sizes can be used to deliver attackers, explosives, or hazardous materials; they can also be used as weapons.

Cyber Attack

Terrorists can infiltrate data processing, transfer, and storage systems to cause economic and operational damage. Supervisory control and data acquisition (SCADA) systems can be infiltrated to operate infrastructure systems in a manner that can cause damage and inflict on-site and off-site casualties.

Sabotage

The disruption, damage, or destruction of a facility through sabotage, the introduction of hazardous materials into the facility, and/or contamination of facility products are of concern. In some cases, sabotage is designed to release hazardous material from a facility into the surrounding area.

Assassination/Kidnapping

Assassinating key personnel or kidnapping individuals and taking hostages have been used in many terrorist acts.

Small Arms Assault

Small arms, including automatic rifles, grenade launchers, shoulder-fired missiles, and other such weaponry, can be aimed at people (e.g., shooting of civilians) or at facilities (e.g., stand-off assault from outside a perimeter fence).

AVAILABLE PROTECTIVE MEASURES

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures are designed to meet one or more of the following objectives:

Devalue Lower the value of a facility to terrorists; that is, make the facility less interesting as a target.

Detect Spot the presence of adversaries and/or dangerous materials and provide responders with information needed to mount an effective response.

Deter Make the facility more difficult to attack successfully.

Defend Respond to an attack to defeat adversaries, protect the facility, and mitigate any effects of an attack.

Many different protective measures are available for deployment at a facility and in the areas surrounding a facility (buffer zones). Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs (e.g., redundancy). In general, applicable protective measures can be grouped into several broad categories as shown in Table 1. The table is intended to be illustrative rather than comprehensive. In addition to these generally applicable measures, some protective measures are specifically oriented toward higher education institutions. These measures are discussed later.

Table 1 Categories of Generally Applicable Protective Measures

Protective Measure Type	Protective Measure Description and Examples
Access Control	**Control of employees/visitors/vehicles entering a facility site or a controlled area in the vicinity of a facility**
	Controlled entrances (e.g., doors, entryways, gates, locks, turnstiles, door alarms)
	Control of material (e.g., raw materials, finished products)
	Secured perimeters (e.g., fences)
	Restricted access areas (e.g., key assets; roofs; heating, ventilation, and air-conditioning [HVAC] systems)
	Access identification (e.g., employee badges, biometric identification)
	Signage
Barriers	**Physical barriers and barricades**
	Walls
	Fences (e.g., chain link, barbed wire)
	Earthen banks and berms (e.g., for blast protection)
	Screens and shields (e.g., for visual screening)
	Vehicle barriers (e.g., bollards, Jersey barriers, planters, tire shredders, vehicles used as temporary barriers)
Monitoring and Surveillance	**Use of equipment to monitor movement of people and material in and around a facility and to detect contraband**
	Closed-circuit television (CCTV) cameras (e.g., fixed, pan-tilt-zoom, recording capability)
	Motion detectors
	Fire and smoke detectors
	Heat sensors
	Explosives detectors
	Chemical agent detectors (chemical warfare agents, toxic industrial chemicals)
	Biological agent detectors
	Radiological agent detectors
	Metal detectors
	Night-vision optics (infrared, thermal)
	Lighting (buildings, perimeter, permanent/temporary)
Communications	**Communication capability within a facility and between a facility and local authorities**
	Telephone (land line, cell, satellite)
	Radio
	Interoperable equipment (within facility, with local jurisdictions)
	Redundant and backup communication capabilities
	Data lines (Internet, dedicated lines)
Inspection	**Inspection of people, vehicles, and shipments for explosives, chemical/biological/radiological agents**
	Personnel searches (including employees, visitors, contractors, vendors)
	Vehicle searches (cars, trucks, delivery vehicles, boats)
	Cargo and shipment searches (trucks, containers, railcars, marine vessels, aircraft)
	Trained and certified dogs
	X-ray screening
Security Force	**Personnel assigned security responsibility**
	Force size
	Equipment (weapons, communication gear, vehicles, protective clothing and gear, specialized incident-response gear)
	Training (basic, specialized)
	Operational procedures (patrols, checkpoints, spot checks, standard operating procedures)
	(Continued on following page.)

Table 1 Categories of Generally Applicable Protective Measures

Protective Measure Type	Protective Measure Description and Examples
Cyber Security	**Protection of computer and data systems**
	Firewalls
	Virus protection
	Password procedures
	Information encryption
	Computer access control
	Intrusion detection systems
	Redundant and backup systems
Security Program	**Procedures and policies**
	Employee background checks
	Employee security awareness and training
	Visitor control and monitoring
	Security reporting system
	Operations security plan
	Coordination among facility, local law enforcement, state agencies, and federal agencies
Incident Response	**Procedures and capability to respond to an attack**
	Emergency response plan
	Emergency response equipment
	Emergency response personnel
	Emergency response training and drills
	Shelter facilities
	Communication with the public
Personnel Protection	**Procedures to protect personnel from attack**
	Protection for high-profile management personnel (e.g., guard escorts, schedule and route changes)
	Protection for employees (e.g., alerts, reduced travel and business activity outside facility)
Infrastructure Interdependencies	**Protection of site utilities, material inputs, and products**
	Utilities (e.g., electric power, natural gas, petroleum products, water, telecommunications)
	Inputs (e.g., raw materials, parts)
	Outputs (e.g., finished products, intermediate products)

IMPLEMENTATION OF PROTECTIVE MEASURES

Some protective measures are designed to be implemented on a permanent basis to serve as routine protection for a facility. Such measures are sometimes referred to as “baseline countermeasures.” Other measures are implemented or increased in their application only during times of heightened alert. The implementation of any protective measure at any time involves the commitment of resources in the form of people, equipment, materials, time, and money. Facility owners, local law enforcement, emergency responders, and state and local government agencies need to coordinate and cooperate on what measures to implement, how extensive they should be, and how long they should be kept in force in order to maximize security while staying within the bounds of available resources.

To assist in the decision process, the U.S. Department of Homeland Security (DHS) has developed the color-coded Homeland Security Advisory System (HSAS) to communicate with public safety officials and the public at large so that protective measures can be implemented or expanded to reduce the likelihood or impact of an attack. Table 2 shows the HSAS alert levels.

Table 2 Homeland Security Advisory System Alert Levels

Alert Level		Description
Red	SEVERE	Severe risk of terrorist attack
Orange	HIGH	High risk of terrorist attack
Yellow	ELEVATED	Significant risk of terrorist attack
Blue	GUARDED	General risk of terrorist attack
Green	LOW	Low risk of terrorist attack

When the available intelligence allows, the HSAS alerts are supplemented by information on the threat stream(s) most likely to be used by terrorists. This information may or may not be very specific, may or may not identify geographical areas of concern, and may or may not offer a time period when attacks might be expected. This level of uncertainty is inherent in dealing with terrorist threats and must be factored into decisions on committing resources to the implementation of protective measures.

In addition to the HSAS, some infrastructure owners, industry associations, and information sharing and analysis centers (ISACs) have developed their own alert classification schemes tailored to specific critical infrastructure or key asset segments. For example, the American Association of State Colleges and Universities has produced a paper entitled *Addressing the Challenge of Campus Security* [http://www.aascu.org/policy/special_report/security.htm], which discusses prevention and deterrence measures that universities can take to enhance campus security. Likewise, the National Association of State Universities and Land-Grant Colleges (NASULGC) co-hosted a Campus Security Summit with the DHS's Office of Domestic Preparedness in 2003. (Results are summarized in a newsletter entitled *Prevention Strategies Highlighted at Campus Security Summit* [http://www.nasulgc.org/whatsnew/newsline/2003/campus_security.pdf].)

Many higher education institutions are located on campuses that include a variety of buildings and other facilities. Among the structures found on a campus are libraries, lecture halls, laboratories, student housing areas, administration buildings, book stores, parking areas, auditoriums, gymnasiums, and cafeterias or other dining areas. Large and mid-size campuses can also have stadiums and arenas, small power plants, communication hubs, and other utility-type structures. Many campuses have park-like settings for students, faculty, and others in which to study or relax. While many campuses are physically distinct entities, urban campuses can be bisected by city streets. Often buildings and other facilities are not physically separated from the rest of the urban area and may be identical to contiguous noninstitutional edifices.

Not all higher education institutions are located on campuses. Smaller institutions may be located in a single building. In some cases, they may be the sole occupant, while in other instances, they may be a tenant in a multipurpose building that houses a variety of businesses and other organizations.

University and college stadiums, arenas, performing arts centers, and libraries are similar to off-campus and non-academic-institution counterparts. These facilities are not discussed in detail in this document. Likewise, protective measures related to power plants and other nonacademic facilities are not addressed here. This document focuses primarily on higher education institutions located on distinct campuses.

Exhibits 1–5 provide information and assistance to facility owners, local law enforcement, and state and local homeland security agencies in making decisions on how to increase security at higher education institutions on the basis of the HSAS alert levels. These suggested measures are collated from infrastructure-specific guidance and from experience in a number of localities across the country. The following should be noted regarding the suggested protective measures:

- These measures are intended as a guide; they are not a requirement under any regulation or legislation.

- The suggested steps are additive, meaning that higher threat levels should also include those measures given for lower threat levels.

- These suggestions are based on practices used by facilities across the nation. The ability to implement them at a specific facility will vary.

- These suggestions should not be viewed as a complete source of information on protecting facilities. Facility managers and local security personnel should consider the full range of resources available, as well as the specific nature of the threats, when responding to changes in threat condition levels.

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green

Measures put in place under this threat level can be considered to be "baseline countermeasures" that are in place under all conditions. Infrastructure-specific guidelines provide detailed information on specific measures (see References 1–22), which are not repeated here. The following list provides a brief summary of the major types of protective measures suggested for implementation.

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
		x		Define controlled areas requiring security (e.g., academic buildings; housing areas; laboratories; control rooms; maintenance areas; and heating, ventilation, and air-conditioning [HVAC] systems).	Institution
		x		Secure entrances to controlled areas (e.g., doors, entryways, gates, locks, turnstiles, and door alarms).	Institution
		x		Secure hazardous materials (e.g., laboratory chemicals and specimens, fuel).	Institution
x		x		Provide appropriate signage.	Institution
	x	x		Control student, faculty, and employee identification and access to controlled areas through use of picture badges.	Institution
	x	x		Control visitor identification and access to controlled areas through use of pass or badge.	Institution
	x	x		Control contractor, vendor, and temporary personnel identification and access to controlled areas through use of pass or badge.	Institution
		x		Grant access only to authorized personnel when buildings are locked.	Institution
				Barriers	
		x		Provide adequate perimeter fencing or walls around controlled access areas.	Institution
		x	x	Place physical barriers outside sensitive buildings.	Institution
				Monitoring and Surveillance	
	x	x		Provide adequate lighting campuswide.	Institution
	x			Provide intrusion detection systems at all controlled facilities.	Institution
	x	x		Provide video surveillance systems campuswide.	Institution
	x	x		Establish a campus-based community watch program similar to block or neighborhood watch programs.	Institution
				Communications	
		x	x	Establish close ties with local, state, and federal agencies, including the agent in charge of the nearest FBI field office and the regional Joint Terrorism Task Force.	Institution; local, federal, and state law enforcement agencies
		x	x	Develop liaison with local, federal, and state law enforcement emergency response teams to enhance information exchange, clarify emergency response, track threat conditions, and support investigations.	Institution; local, federal, and state law enforcement agencies
	x	x		Develop liaison with educational information-sharing organizations, such as the American Association of State Colleges and Universities and the National Association of State Universities and Land-Grant Colleges.	Institution, appropriate organizations
			x	Develop communication process with general public regarding situations and incidents.	Institution; local government
		x	x	Establish a campuswide emergency telephone system.	Institution
				Inspection	
	x	x	x	Inspect campus lightning protection systems and ensure all wires and cables are connected.	Institution
		x	x	Check and inspect emergency building systems, fire alarms, emergency generators, and exit lights.	Institution
	x	x	x	Check outdoor air intakes of HVAC systems to ensure they are protected.	Institution
	x	x	x	Locate outdoor air intakes of HVAC systems in or on a building wall at least at second-story level, preferably higher. For rooftop or ground-level intakes that cannot be modified, establish a security zone to limit access.	Institution

(Continued on following page.)

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green

Measures put in place under this threat level can be considered to be "baseline countermeasures" that are in place under all conditions. Infrastructure-specific guidelines provide detailed information on specific measures (see References 1–22), which are not repeated here. The following list provides a brief summary of the major types of protective measures suggested for implementation.

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Security Force	
	x	x	x	Maintain adequately staffed and equipped security force.	Institution
	x	x	x	Conduct regular patrols of the campus, buildings, and facilities.	Institution
	x		x	Conduct drills and exercises for security force.	Institution
	x		x	Train and prepare security force to recognize potentially dangerous situations on and around campus.	Institution
	x	x		Assign campus security officers as liaisons with international student groups. On some state university campuses, security force officers are provided by the state police. Likewise, local law enforcement agencies may provide security force officers at other public higher education institutions.	Institution, local and state law enforcement agencies
				Cyber Security	
	x	x	x	Develop secure information technology network architecture.	Institution
		x	x	Control access to information technology systems (on-site, remote access).	Institution
			x	Maintain backup information technology systems.	Institution
	x	x	x	Locate mission-critical system facilities in a secure location that is locked and restricted to authorized personnel only.	Institution
	x	x	x	Physically secure computers in an area inaccessible to unauthorized users.	Institution
	x	x	x	Check the credentials of external information technology contractors.	Institution
x	x	x	x	Ensure that operating systems are updated with current security patches.	Institution
x	x	x	x	Use and regularly update anti-virus software.	Institution
	x	x	x	Control access to critical computer hardware, wiring, displays, and networks by rules of least privilege.	Institution
		x	x	Document system configurations (e.g., hardware, wiring, displays, and networks) of critical systems. Govern installations and changes to those physical configurations by a formal change management process.	Institution
	x	x	x	Implement a system of monitoring and auditing physical access to critical computer hardware, wiring, displays, and networks (e.g., badges, cameras, and access logs).	Institution
				Security Program	
	x		x	Invite local, state, and federal law enforcement officers to campus to help them become familiar with the institution, its leadership, and the complexity of its operations.	Institution, , local and state law enforcement agencies
			x	Become involved in regional homeland security planning.	Institution
x	x	x	x	Conduct threat analysis, vulnerability assessment, consequence analysis, and risk assessment.	Institution
x	x	x	x	Establish threat-assessment teams and develop checklists for each level of threat identified by the DHS.	Institution
x	x	x	x	Develop a comprehensive security plan, policies, and procedures.	Institution
	x	x		Conduct employee background screening.	Institution
x	x	x	x	Refine and exercise as appropriate preplanned protective measures.	Institution
x	x	x	x	Ensure that all facilities are assessed for vulnerabilities to emergencies and terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities.	Institution
	x	x	x	Disseminate written instructions for use by personnel in emergency situations.	Institution
	x	x	x	Develop a security awareness program for employees, students, and faculty.	Institution

(Continued on following page.)

Exhibit 1 Protective Measures Implemented at HSAS Threat Level Green

Measures put in place under this threat level can be considered to be "baseline countermeasures" that are in place under all conditions. Infrastructure-specific guidelines provide detailed information on specific measures (see References 1–22), which are not repeated here. The following list provides a brief summary of the major types of protective measures suggested for implementation.

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Incident Response	
			x	Develop a unified command plan with the local government and law enforcement agencies.	Institution, local government, and local law enforcement agencies
			x	Establish a management team responsible for directing the development and implementation of a campus emergency operations plan.	Institution
			x	Maintain an adequately staffed, equipped, and trained emergency response team.	Institution
			x	Conduct drills and exercises for emergency response team.	Institution
			x	Establish an Emergency Operations Center.	Institution
			x	Conduct fire and other safety drills for the entire campus community.	Institution
				Personnel Protection	
		x	x	Provide safety and security briefing to all students, faculty, and employees.	Institution
x		x	x	Disclose information to the campus community about crime on and around the campus in accordance with the provisions of the "Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act."	Institution
x	x	x	x	Ensure personnel receive proper training on personal protective measures.	Institution
				Infrastructure Interdependencies	
			x	Provide adequate utility services.	Institution
	x	x	x	Provide backup for critical utility services.	Institution
	x	x	x	Provide adequate security for utility services.	Institution

Exhibit 2 Protective Measures Implemented at HSAS Threat Level Blue

Ensure measures taken for lower alert level are reviewed and reinforced, as needed. Review the measures listed in the higher alert levels to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
	x	x	x	Control entrance to sensitive areas through manned security checkpoints.	Institution
		x		Secure buildings, rooms, and storage areas not in normal use.	Institution
	x	x		Reinforce use and display of ID badges at all times.	Institution
		x		Limit vehicle access to controlled areas to essential vehicles only.	Institution
				Barriers	
		x		Review security hardware on doors, locks, and windows.	Institution
		x		Check fences and lighting.	Institution
			x	Check HVAC shutoff and intake controls.	Institution
				Monitoring and Surveillance	
	x	x		Check operation of CCTV system.	Institution
				Communications	
	x	x	x	Check facility communication systems.	Institution
	x	x	x	Ensure that radio/phone contact with local law enforcement works.	Institution; local law enforcement
	x			Ensure alarm systems work.	Institution
	x	x	x	Check communications with designated response or command locations.	Institution
x	x	x	x	Provide the public with information so people can act appropriately.	Institution
	x		x	Check security radios and ensure batteries are readily available.	Institution
				Inspection	
	x	x		Conduct security spot checks of individuals entering controlled areas.	Institution
	x	x		Conduct security spot checks of vehicles entering controlled areas.	Institution
		x	x	Check and inspect emergency building systems, fire alarms, emergency generators, and exit lights.	Institution
				Security Force	
	x	x	x	Review existing countermeasures and operational procedures to ensure adequate guard allocation and access control procedures.	Institution
	x	x	x	Conduct comprehensive patrols of entire campus on each shift.	Institution
				Cyber Security	
	x			Increase monitoring of all external network connections.	Institution
			x	Ensure coordination with supporting telecommunication restoration priorities and plans.	Institution
			x	Increase the frequency of mission-critical data backup.	Institution
				Security Program	
	x	x		Maintain vigilance of changes in vendor personnel with site access.	Institution
			x	Conduct tabletop emergency response exercises.	Institution, local government
				Incident Response	
		x	x	Put key personnel on call who can implement security plans and seal off areas.	Institution
			x	Review contingency, evacuation/relocation plans, and emergency response procedures/manuals.	Institution
			x	Check plans for implementation to next threat level.	Institution
			x	Conduct pre-incident liaison and planning with federal or other weapons of mass destruction (WMD) response organizations, as appropriate.	Institution, local law enforcement, WMD response organizations

(Continued on following page.)

Exhibit 2 Protective Measures Implemented at HSAS Threat Level Blue

Ensure measures taken for lower alert level are reviewed and reinforced, as needed. Review the measures listed in the higher alert levels to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Personnel Protection	
	x	x		Advise personnel on rising threat.	Institution
	x	x		Reinforce personal security awareness.	Institution
		x	x	Consider enhanced security measures for high-profile administrators and faculty members.	Institution
				Infrastructure Interdependencies	
		x	x	Check barriers around utility supply points (e.g., fences, locks).	Institution

Exhibit 3 Protective Measures Implemented at HSAS Threat Level Yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher alert levels to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
	x	x	x	Establish a single point of access for each critical facility and institute 100% identification checks.	Institution
	x	x	x	Increase administrative inspections of persons and their possessions entering critical facilities.	Institution
		x		Limit access to critical facilities to an absolute minimum.	Institution
		x		Escort all visitors and nonemployees within critical facilities at all times.	Institution
		x		Prevent vehicles from parking within 25 meters of buildings and other structures.	Institution
		x		Consider centralized parking.	Institution
		x		Establish manned checkpoints and positively identify all vehicles allowed onto campus.	Institution
		x		Require that a host be contacted to authorize visitor entry to critical facilities.	Institution
		x		Limit number of vehicle entry points onto campus.	Institution
				Barriers	
		x	x	Assess adequacy of physical barriers outside sensitive buildings and proximity of parking.	
				Monitoring and Surveillance	
	x	x		Assess adequacy of video monitoring.	Institution
	x	x		At beginning and end of each day, inspect interior/exterior of buildings and storage areas in regular use.	Institution
	x	x		Increase building spot checks.	Institution
	x	x		Provide CCTV video feed to local law enforcement.	Institution, local law enforcement
	x			Check HVAC filtration, any detectors and monitors, and alarm systems.	Institution
	x	x	x	Increase surveillance of critical locations.	Institution
				Communications	
		x	x	Ensure adequacy of emergency alert and communication system for students, faculty, staff, and visitors.	Institution
		x	x	Review institutional crisis communications plan, including parent and stakeholder communications.	Institution
	x	x	x	Enhance interface with local law enforcement, safety, and related emergency groups.	Institution, local law enforcement
	x	x		Conduct additional briefings for administrative personnel, faculty, and students.	Institution
			x	Provide backup power source for communications equipment.	Institution
				Inspection	
	x	x		Increase physical checks of critical facilities during periods of increased alert.	Institution
	x	x		Randomly inspect visitors' briefcases, backpacks, and other packages.	Institution
	x	x		Increase frequency of personnel spot checks.	Institution
	x	x		Increase vehicle spot checks.	Institution
	x			Raise awareness regarding delivery of suspect mail and packages.	Institution
	x			Enhance mail inspection procedures.	Institution
				Security Force	
	x	x	x	Consider guard reinforcement, and ensure that guards are adequately trained in procedures.	Institution
	x	x	x	Expand roving/motorized patrols to outer perimeter.	Institution
	x	x		Have security guards visually inspect the interior and exterior of all vehicles entering the main gate (a brief visual inspection by walking around the vehicle and looking inside cab and cargo hold, no undercarriage inspections).	Institution
				Cyber Security	
	x			Increase frequency of cyber system monitoring.	Institution

(Continued on following page.)

Exhibit 3 Protective Measures Implemented at HSAS Threat Level Yellow

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher alert levels to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Security Program	
x	x	x	x	Assess if preplanned protective measures need refinement.	Institution
x	x	x	x	Implement, as appropriate, contingency and emergency response plans.	Institution
				Incident Response	
			x	Ensure all personnel responsible for countermeasures are on call.	Institution
			x	Review campus lockdown/shutdown plans.	Institution
			x	Ensure operability of Emergency Operations Center.	Institution
				Personnel Protection	
	x	x		Update personnel on rising threat.	Institution
		x	x	Implement additional security measures for high-profile administrators and faculty.	Institution
				Infrastructure Interdependencies	
		x		Add barriers to utility supply points.	Institution
	x	x	x	Increase patrols at utility supply points.	Institution, local law enforcement

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher alert level to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
x		x		Establish security checkpoints to keep adversaries distant from the facility; consider road closures.	Local law enforcement
		x		Strictly enforce access control.	Institution
		x		Restrict access to facility to that essential for operational purposes only.	Institution
		x		Enforce centralized parking away from facilities and arrange security for those vehicles.	Institution
		x		Consider restricting parking to locations outside the facility.	Institution, local law enforcement
		x		Require visitors to be escorted at all times in sensitive areas.	Institution
		x		Restrict deliveries to daytime hours only.	Institution
		x		Cancel or delay nonvital contractor work.	Institution
		x		Require vendors and contractors to be on preapproved list.	Institution
		x		Restrict threatened facility access to essential personnel only.	Institution
				Barriers	
	x	x		Secure and regularly inspect all buildings, rooms, and storage areas in regular use.	Institution
		x		Erect barriers and obstacles to control vehicle flow through the campus.	Institution, local law enforcement
		x		Erect Jersey barriers at critical assets.	Institution, local law enforcement
				Monitoring and Surveillance	
	x	x		Install additional temporary lighting at critical assets.	Institution
				Communications	
	x	x	x	Provide daily security and awareness briefings to administrative staff.	Institution
				Inspection	
	x	x		Check/screen all deliveries.	Institution
	x	x		Increase frequency of random inspections of visitors' briefcases, backpacks, and other packages.	Institution
	x	x		Search all vehicles and contents before they are allowed to enter the campus.	Institution
				Security Force	
	x	x	x	Increase numbers of security guards and patrol activities.	Institution
		x	x	Consider deployment of law enforcement personnel and instruct guards on procedural implications. Use law enforcement officers during daylight hours as available.	Institution, local law enforcement
		x	x	Provide additional weapons and equipment to security force.	Institution
	x	x		Use an explosives-detecting canine unit.	Institution
				Cyber Security	
		x		Reduce number of people authorized to access computer systems.	Institution
		x		Disable access to Internet and other portals that might allow unauthorized access.	Institution
		x	x	Implement more frequent backup procedures.	Institution
				Security Program	
		x		Prohibit vehicles from leaving site without pass.	Institution
		x	x	Provide police escort for vehicles transporting hazardous material leaving facility and traversing surrounding community.	Local law enforcement
		x		Evaluate the risk of public events and take the necessary precautions	Institution
x	x	x	x	Prepare to execute contingency procedures.	Institution
				Incident Response	
			x	Ensure all personnel responsible for implementing countermeasures are immediately available.	Institution

(Continued on following page.)

Exhibit 4 Protective Measures Implemented at HSAS Threat Level Orange

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Review the measures listed in the higher alert level to determine which measures should be implemented on the basis of the current threat, and consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
			x	Add firefighter and emergency medical personnel to shifts.	Local government
			x	Activate Emergency Operations Center.	Institution
				Personnel Protection	
	x	x		Update personnel on escalating threat.	Institution
			x	Verify shelter-in-place procedures and equipment.	Institution
			x	Ensure that best available filtration is being used for existing HVAC configuration.	Institution
				Infrastructure Interdependencies	
		x		Add barriers to critical utility supply points.	Institution
		x	x	Where possible, provide additional backup utility supplies (e.g., backup generators).	Institution
	x	x	x	Provide additional monitoring of utility supply points.	Institution, local law enforcement

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
				Access Control	
x		x		Coordinate with local authorities regarding closing of public roads and facilities.	Institution, local law enforcement
		x		Allow no visitors.	Institution
	x	x		Allow no nonessential vehicles onto campus. Thoroughly search all vehicles entering campus, including undercarriage.	Institution
		x		Monitor, redirect, or constrain transportation systems.	Institution
		x	x	Close facilities.	Institution
				Barriers	
		x		Deploy temporary barriers at all key assets.	Institution
			x	Move objects that could become projectiles 25 meters away from buildings.	Institution
				Monitoring and Surveillance	
	x	x		Make frequent checks of all exterior areas of the campus, including parking.	Institution
	x	x		Leave lighting on 24/7.	Institution
				Communications	
			x	Test communications and notification procedures.	Institution
			x	Advise site management of potential implementation of evacuation/relocation plan.	Institution
			x	Conduct daily briefings with local law enforcement on threat condition.	Institution, local law enforcement
				Inspection	
	x	x		Search all persons prior to entering the campus.	Institution
	x			Process mail off site.	Institution
		x	x	Pick up and store all loose items, such as trash cans, benches, newspaper racks, cigarette urns, traffic cones, barriers, freestanding signs, and recyclable containers or any items not permanently attached to a structure.	Institution
				Security Force	
	x	x		Patrol entire campus continually.	Institution
		x	x	Augment security guards with law enforcement where feasible. Arrange to have law enforcement officers on site 24 hours as available.	Institution, local law enforcement
		x	x	Consider armed guards.	Institution
		x	x	Deploy mobile command post on campus.	Institution, law enforcement
	x	x	x	Increase or redirect personnel to address critical emergency needs.	Institution
				Cyber Security	
		x		Restrict computer access to essential personnel only.	Institution
	x	x	x	Increase computer security levels to maximum.	Institution
				Security Program	
	x	x		Verify identity of all personnel working in critical areas.	Institution
				Incident Response	
			x	Check all available emergency equipment.	Institution
			x	Prepare Emergency Operations Center for use.	Institution, local government
			x	Add firefighter and emergency medical personnel to shifts.	Local government
			x	Assign emergency response personnel.	Institution
	x	x	x	Pre-position and mobilize specially trained teams or special resources.	Institution
				Personnel Protection	
	x	x		Update personnel on escalating threat.	Institution
			x	Establish positive control on facility air intakes. Prevent all unfiltered air from reaching manned spaces.	Institution

(Continued on following page.)

Exhibit 5 Protective Measures Implemented at HSAS Threat Level Red

Ensure measures taken for lower alert levels are reviewed and reinforced, as needed. Consider implementation of the following protective measures:

Devalue	Detect	Deter	Defend	Protective Measures	Measure Implemented by
			x	Ensure that security force and emergency responders have breathing apparatus, if appropriate, and are prepared to evacuate or shelter in place.	Institution
				Infrastructure Interdependencies	
	x	x	x	Provide continuous guard at utility supply points.	Institution, local law enforcement

USEFUL REFERENCES

1. Security on Campus, Inc., Web site [http://www.securityoncampus.org/].

2. American Association of State Colleges and Universities, Web site [http://www.aascu.org/policy/special_report/security.htm].

3. American Association of State Colleges and Universities, *Addressing the Challenge of Campus Security* [http://www.aascu.org/policy/special_report/security.htm].

4. National Association of State Universities and Land-Grant Colleges, Web site [http://www.nasulgc.org].

5. National Association of State Universities and Land-Grant Colleges, *Prevention Strategies Highlighted at Campus Security Summit* [http://www.nasulgc.org/whatsnew/newsline/2003/campus_security.pdf].

6. U.S. Department of Education, Office of Postsecondary Education, Campus Security, Web site [http://www.ed.gov/admins/lead/safety/campus.html].

7. Rivard, N., *On the Campus: Rethinking Security*, University Business [http://www.universitybusiness.com/page.cfm?p=77].

8. Angelo, J.M., *Caught on Camera*, University Business [http://www.universitybusiness.com/page.cfm?p=700].

9. Pantera, M.J., III, *Planning Is Key to Locking Down Security*, NCAA News [http://www.ncaa.org/news/2003/20030818/editorial/4017n30.html].

10. Pantera, M.J., III, et al., “Best Practices for Game Day Security at Athletic and Sport Venues,” *The Sports Journal* [http://www.thesportjournal.org/2003Journal/Vol6-No4/security.asp].

11. Springfield College, *Game Day Security Operations Checklist* [http://www.thesportjournal.org/2003Journal/Vol6-No4/documents/Checklist-GameDaySecurity.pdf].

12. Congressional Research Service Report, *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education* [http://www.fas.org/irp/crs/RL31354.pdf].

13. Association of American Universities, *Homeland Security Issues* [http://www.aau.edu/homeland/homelandSecurityIssues.cfm].

14. International Association of Campus Law Enforcement Administrators, Web site [http://www.iaclea.org/].

15. Denison University, *Universities throughout North America with Security Sites.* Granville, OH [http://www.denison.edu/ sec-safe/others.html].

16. University of Kansas, *Emergency Plan* [http://www.ku.edu/~kucops/security/UnvE-Plan2.03.htm.]

17. Drexel University, *Emergency Response Plan* [http://www.drexel.edu/admin/publicsafety/response/level.htm].

18. Federal Emergency Management Agency, *FEMA Toolkit—Appendix D, Cyber-Terrorism* [http://www.fema.gov/txt/onp/toolkit_app_d.txt].

19. Florida Atlantic University, *FAU Broward Campuses Emergency Operations Plan* [http://www.broward.fau.edu/phyplant/EOP%20Fort%20Lauderdale.pdf].

20. Adams, J.A., LTC (ret.), and J. Sinai, *Protecting Schools and Universities from Terrorism; A Guide for Administrators and Teachers*, ASIS International [http://www.asisonline.org/store/detail.xml?id=2003].

21. Bahnfleth, W.P., *Reducing Building Vulnerability: Recent Guidance Documents*, HPAC Engineering [http://www.hpac.com/microsites/hsb/bahnfleth_hsbsup/bahnfleth_hsbsup.htm#physical].

22. University of Mary Washington, *Information Technologies Security Program* [http://www.umw.edu/policies/itsecurityprogram/].

Note: Information presented here is subject to copyright laws and other terms of use as set forth in the respective references.